Quarantine Release Portal

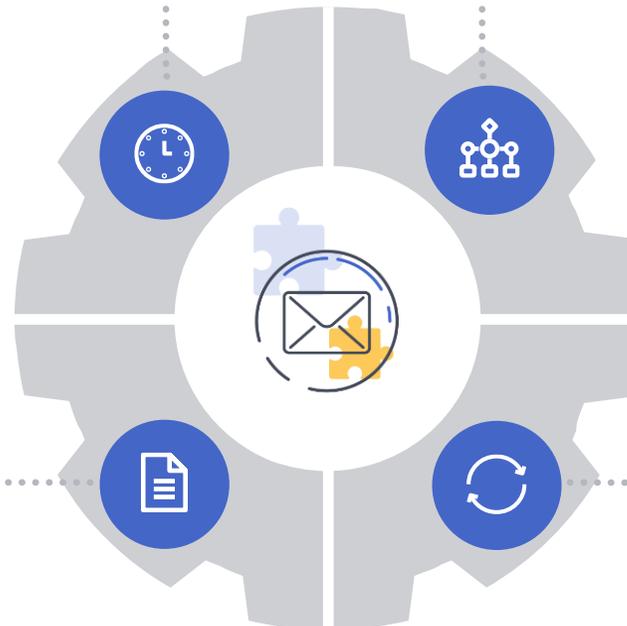## Protirus Information Protection eXtensions

GAIN CONTROL OF YOUR DLP INCIDENTS BY HANDING POWER BACK TO YOUR BUSINESS

Self-service Quarantine Release Portal

Users request their manager's approval for the release of emails that have been improperly blocked; the request is accompanied by specific business explanation. Users can track the status of the request through an easy-to-use portal.

Target Quick & Accurate Remediation Actions

Respecting your organisation's structure, the process allows a user's manager to use their understanding of the user's role and corresponding business requirements, to perform remediation actions, such as release quarantined mails or escalate to security for investigation.

Configure Notifications With Multi-Lingual Support

Configure email notifications in the language of the end-user's choice to orchestrate the process

Secure and Integrated

Builds on your Symantec DLP investment and integrates with third-party security access management systems, including SAML Single Sign On, CyberArk and other major SIEMs.

PROTIRUS

PIPeX Quarantine Release Portal

How It Works

Policy Violation

An employee performs an action that is not compliant with Company policy. An incident is instantly raised

Employee Justification

Through the Quarantine Release Portal, the employee provides the manager additional context on the intent of the action that was flagged

Quarantine and Manager Notification

The data in question is quarantined and the manager notified. The manager has the responsibility of determining if this action corresponds to expected behaviour

Manager Determination

The manager now has the information needed to make an informed decision on the approval or security escalation of the action

Watch our video online:
https://www.youtube.com/watch?v=2ftonxee450&

PROTIRUS

PIPeX Quarantine Release Portal

How It Addresses Your Incident Management Challenges

Challenges

Solutions

Central **security teams** have a **limited** number of **people** and limited **time** to respond to DLP incidents

Self service portal provides the **local teams** the ability to **make decisions themselves**

DLP requires the definition of **rules**. These rules apply globally, at a country level or even to a local team. No matter how granular these rules are, there will always be **users** that are the **exception** at a given time

Local teams have the **necessary business context** to understand what constitutes valid activity or transgression. The record of this **knowledge over time** allows the **tuning of the policy** rules, resulting in more accuracy and less incidents over time

---

There's an inevitable **trade off** between **productivity** and **security**. E.g. when a transfer of data to the outside raises a flag and is halted, the **business cannot afford** for it to be **held up** until the security team reviews the incident

You **do not compromise security**, as issues are temporarily held in quarantine, and **productivity is not compromised** as the local teams have control of the approval of their own incidents

PROTIRUS